

May 10, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

}

Case No. 23 MJ 85

The property located at 6554 N Sidney Place,
Apt. 202, Glendale, WI 53209.

}

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Section 371, 1344, & 1343	Conspiracy, Wire Fraud, & Bank Fraud

The application is based on these facts:

See Attached Affidavit

Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SA Jacob Dettmerring, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: 5/10/2023

William E. Duffin

Judge's signature

Hon. William E Duffin, U.S. Magistrate Judge

Printed name and title

City and state: Milwaukee, WI

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Jacob A. Dettmerring, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 6554 N Sidney Place, Apt. 202, Glendale, WI 53209, hereinafter “PREMISES,” further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since January 7, 2018. I was assigned to the FBI Capital Area Gang Task Force (CAGTF) in Baton Rouge, Louisiana from June 15, 2018, to April 1, 2020. Since April 1, 2020, I have been assigned as the Task Force Coordinator for the Milwaukee Area Safe Streets Task Force (MASSTF). Since 2018, I have investigated violations of federal law, directed drug and street gang investigations, obtained and executed search and arrest warrants related to the distribution of illegal narcotics, and debriefed confidential informants and cooperating defendants. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

3. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and

debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

4. The facts in this affidavit come from my training and experience, my review of documents and information obtained from other agents/law enforcement officers. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Since February 2021, the ATF, Milwaukee Police Department (MPD), Federal Bureau of Investigation (FBI), and Drug Enforcement Administration (DEA) have been investigating identified members of the “Wild 100’s”, a violent street gang in Milwaukee, also known as the “Shark Gang”, including Zariyus DOWL-EAST, (DOB 5/1/1998), among others, for federal firearms offenses and federal program fraud. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Zariyus DOWL-EAST and Brianna EALY have committed violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(g)(1) (possession of a firearm by a felon), 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C. § 1343 (wire fraud),

PROBABLE CAUSE

6. Zariyus DOWL-EAST has emerged as a suspect based upon his connection to the “Wild 100s” street gang. Zariyus DOWL-EAST has been identified as a Wild 100 affiliate via multiple MPD reports, multiple sources of information, and confidential sources. Agents have additionally observed DOWL-EAST photographed with several previously identified Wild 100

members. These individuals exclusively claim affiliation with the gang and do not represent other entities in Milwaukee. Agents quickly learned DOWL-EAST would travel frequently, while flashing large sums of cash.¹ Additionally, DOWL-EAST has allegedly been engaged in multiple instances of COVID-19 fraud. In fact, DOWL-EAST has been observed on his own publicly viewable social media profiles (Instagram: “runupbagsdaily”) posting several pictures of large amounts of cash, firearms, diamonds, jewelry, and other items of value, such as the below:



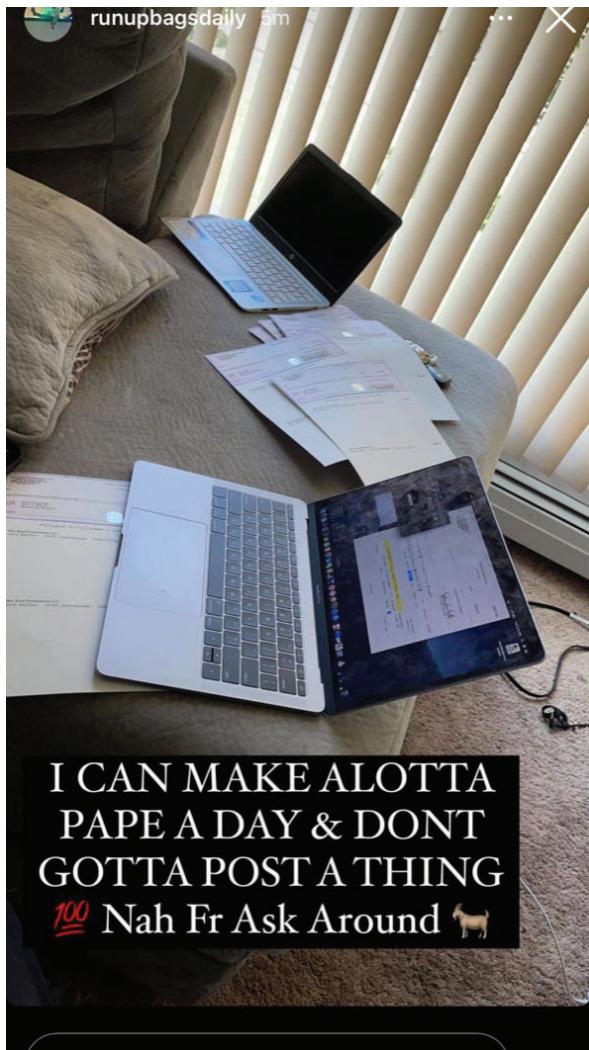
Bank Fraud

¹ According to the Wisconsin Department of Workforce Development (“DWD”), DOWL-EAST has a total of \$425.25 in reported wages from January 1, 2019, through December 31, 2022.

7. From May 2021 to present, case agents have been monitoring the publicly viewable Instagram for DOWL-EAST. DOWL-EAST has been in custody since approximately September of 2022. However, before and since his incarceration, someone has been posting pictures to DOWL-EAST's Instagram page on a regular basis, including pictures advertising/soliciting for help in various fraud schemes, as well as bragging about the same.

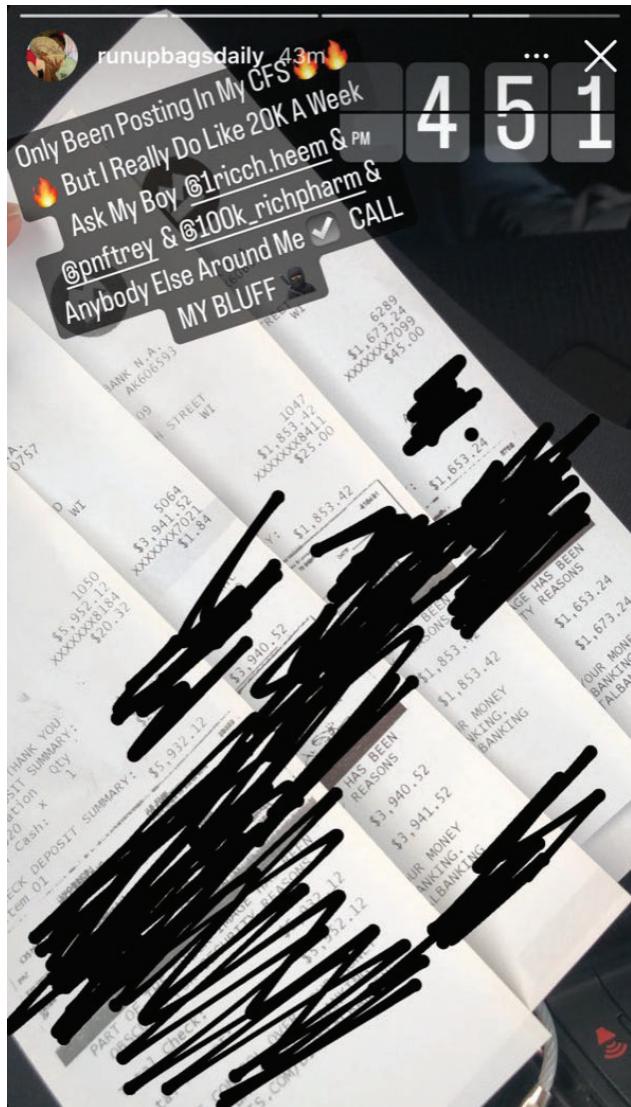
8. Investigators know that bank fraud or ATM scamming is prevalent within the Wild 100s or Shark Gang. Case agents are aware, based upon training and experience, that individuals will engage in a counterfeit check scheme if they are aware that certain banks will make funds available immediately after a deposit. Fraudsters will take advantage of the bank's policy by using an individual's checking account to deposit a counterfeit check, and then immediately withdraw the funds that are made available by the bank before the bank can realize that the check is fraudulent.

9. On June 22, 2021, DOWL-EAST posted a picture which was taken inside of an apartment. The post had two (2) laptops open, sitting on the couch, with a check writing program open on the screen of the computer closest to the camera. Additionally, there were numerous pieces of "check paper" that appeared to be already printed. The caption on the picture was, "I can make a lotta pap a day & Don't gotta post a thing", below that was the caption, "100 Nah Fr Ask Around (goat emoji). Case agents know that DOWL-EAST is referring to himself being the "greatest of all time (GOAT)" at check kiting. A screenshot is set forth below.



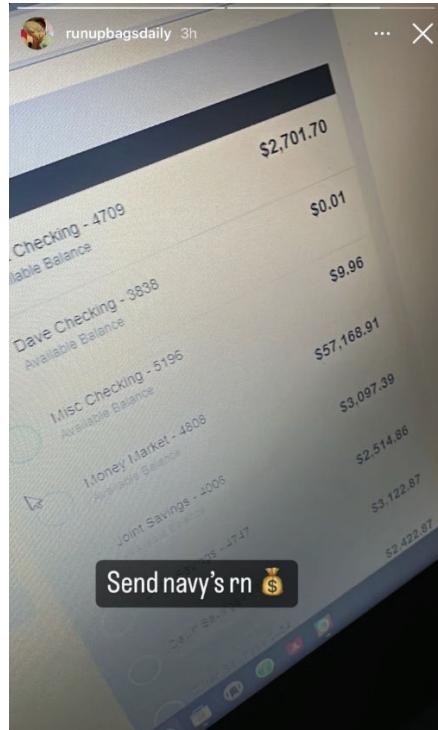
10. On July 12, 2022, DOWL-EAST posted to his Instagram account a picture of four (4) deposit receipts from what appeared to be BMO Bank. The receipts are for four (4) separate accounts showing several deposits. The first account, ending in 8184, showed a deposit of \$5,932.12. The second account, ending in 7021, showed a deposit of \$3,940.52. The third account, ending in 8411, showed a deposit of \$1,853.42. Lastly, the account, ending in 7099,

showed a deposit of \$1,653.24. The caption stated, “Only been Posting In My CFS”, and “But I really do like 20K a week ask my boy @1ricch.heem & @pnftrey & 100k_richpharm & anybody else around me call my bluff”. A screenshot is set forth below.



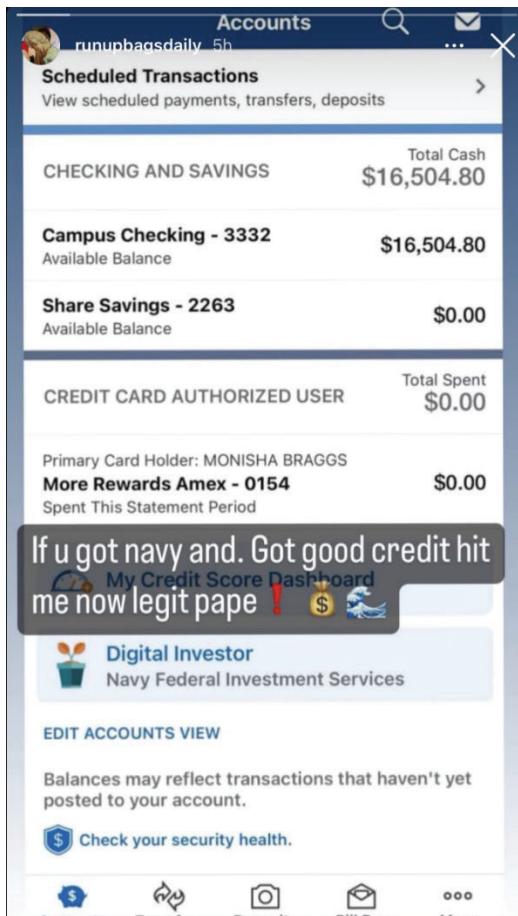
11. However, DOWL-EAST was arrested by West Allis Police Department on

August 18, 2022. DOWL-EAST was arrested for Operating- Flee elude an Officer, great bodily harm, 2nd degree recklessly endangering safety, bail jumping, obstruction of an officer (WAPD Case #22-027385). Although DOWL-EAST was still in custody, on March 3, 2023, the DOWL-EAST Instagram account “runupbagsdaily”, posted a picture of a mobile banking application with numerous linked accounts with a total dollar amount of \$71,038.57. The caption on the picture stated, “Send navy’s rn”. Investigators know this to mean, if a person has a Navy Federal account, send your information so they can participate in the banking scheme. A screen shot is set forth below.



12. On April 8, 2023, the Instagram account “runupbagsdaily”, posted a picture of a

mobile banking application which showed a checking account ending in 3332, with a total amount available of \$16,504.80. The picture had a caption which read, “If you got navy and got good credit hit me now legit pape”. It should be noted that the mobile application shows the primary card holder was in a different person’s name (“Monisha Braggs”). A screenshot is set forth below.



Fraud Related to COVID-19 Relief Programs

13. I have learned from multiple sources, including posts by Wild 100's members on

social media, that the Wild 100's engaged in multiple schemes to defraud unemployment insurance and COVID-19 relief programs. For example, I have seen posts and videos on social media where Wild 100's members use the California EDD system to file fictitious unemployment claims in the names of third parties. They access the site, and file a claim utilizing someone's date of birth, social security number, and phone number. Most individuals split the profits with the person supplying their identity for the claim. The CARES Act established a new program—PUA—to provide unemployment benefits during the COVID-19 pandemic to people who do not qualify for regular unemployment insurance benefits including business owners, self-employed workers, independent contractors, and those with a limited work history who are out of business or have significantly reduced their services as a direct result of the pandemic. Unemployment insurance benefits provided under the PUA program are sometimes referred to as PUA benefits. Each state's unemployment insurance office is responsible for distributing these benefits if available in that state.

14. In many states, PUA is distributed in the form of debit cards that are mailed directly to the beneficiary. The beneficiary may then use the debit card to withdraw the PUA funds from an ATM. Once the claim is approved, the individual committing the fraud will log into EDD and change the mailing address for the loaded debit card to be sent to a Milwaukee address. The individual will then withdraw the money from these loaded debit cards from an ATM and split the profits with the individual for whom they are filing the false claim.

15. Investigators obtained a federal search warrant for the Instagram account

“runupbagsdaily” on October 8, 2021, from the Honorable Magistrate Judge William Duffin in the Eastern District of Wisconsin. Upon review of the Instagram return, Investigators identified several instances of DOWL-EAST attempting to obtain personally protected Information (PII) from individuals via Instagram.

16. On or about December 10, 2020, DOWL-EAST posted a photograph to his Instagram which depicted a laptop screen showing a webpage from California Employment Development Department, which stated “Confirmation-Claim Filed”. The claim was filed using the name “Mariah JOHNSON”. Furthermore, the screen showed numerous other webpage tabs that were minimized. The first was for ID.me, and it stated “your email has been confirmed”. The second showed, “employment development Dep..”, and the third was a webpage for Zillow, which was labeled, “houses for rent in 92102”. A screen shot is set forth below.

Your email has been confirmed. X CONFIRMATION - CLAIM FILED X Employment Development Dept. X Houses For Rent in 92102 - 11

ClaimConfirmation.aspx Help | Benefit Programs Online | Log Out

CA.gov California Employment Development Department

CONFIRMATION - CLAIM FILED

General Information Last Employer Information Employment History Additional Information Summary Confirmation

You Successfully Submitted Your Application

MARIAH JOHNSON, you submitted your application on 12/10/2020. Your confirmation number is 35863464. Keep this number for your records. Your application is being processed and we will contact you by 12/20/2020 with more information. Meanwhile, visit After You File for important steps you must take to make sure your benefit payments are not delayed or denied.

Important: Update your résumé in CalJOBS to avoid a possible delay in your benefits.

It is your responsibility to read the following information.

- Pandemic Unemployment Assistance (PUA)
- Important Notices You Will Receive from the EDD
- Eligibility Determination Interview
- Prior Disqualification or Overpayments
- EDD Debt Card
- Work Search Requirement
- CalJOBS
- Out-of-State Residents
- Reporting Wages
- UI Online
- California Training Benefits
- Rate Your Experience

Pandemic Unemployment Assistance (PUA)

If you are determined to be eligible for PUA, you will receive a Notice of Pandemic Unemployment Assistance Award (DE 429PUA) and an Employment Development Department Customer Account Number notice (DE 5614). You may also receive an email welcoming you to UI Online where you can complete your required certifications for PUA benefits every two weeks. For more information, visit the Pandemic Unemployment Assistance page.

[Back to Top](#)

Important Notices You Will Receive from the EDD

You will receive the following Unemployment insurance claim materials in the mail by 12/20/2020

- Notice of Unemployment Insurance Claim Filed (DE 1181CLMT): Summarizes the information you provided when you filed your claim. This information will be considered accurate unless you contact the EDD within 10 days from the date it was mailed. Failure to report accurate information may result in a disqualification, overpayment, or an overpayment and penalties.
- Notice of Unemployment Insurance Award (DE 429M): Indicates your weekly benefit amount and maximum claim amount which are based on wages paid by your employer(s). Review this award notice for accuracy and contact Unemployment Insurance if the information is inaccurate within 30 days of the mail date of this notice. This notice also provides instructions on your work search requirements.
- Employment Development Department (EDD) Customer Account Number (DE 5614): The EDD Customer Account Number is required to register for UI Online and may be used instead of your Social Security number when speaking to an EDD representative.
- Unemployment Insurance Benefits: What You Need to Know (DE 1275B): A booklet to help you understand the eligibility requirements to receive Unemployment Insurance benefits.

hp

17. On or about June 17, 2021, DOWL-EAST had a communication with “xokeara_”, which he solicited his services for applying for unemployment. In the message, he offers EDD application answers for \$1,000, provide the backdate for \$500 and guarantees \$15,000 in benefits being approved. Investigators know “EDD”, which stands for California’s Employment Development Department. A screenshot is set forth below.



18. Between November 10, 2021 and January 19, 2022, DOWL-EAST had communications with several unknown individuals pertaining to unemployment insurance applications. DOWL-EAST sent a message that stated, “Just find females with bank accounts that wanna make some money extra money... I do all accounts.. I do Edd. SBA. Loans & Etc”. Investigators know DOWL-EAST is referring to unemployment applications and small business administration loans, such as the paycheck protection program (PPP). A screenshot is set forth below.

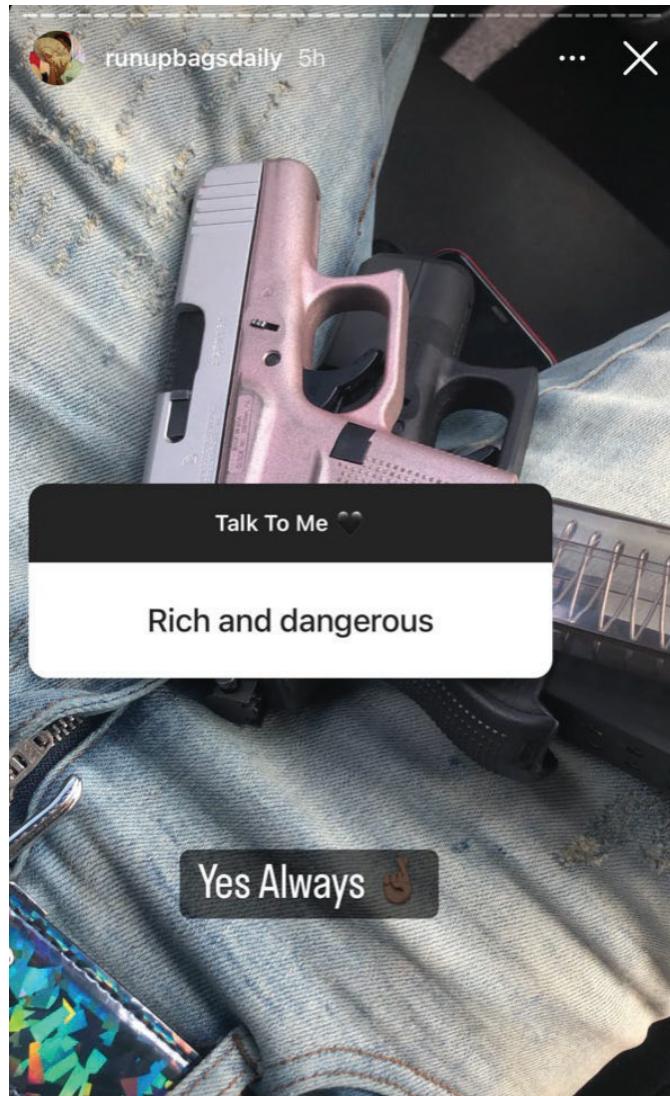
 RunUp BagsDaily > Tiana Dsgood 2021-11-10 17:18:43 (UTC)	Just Find Females With Bank Accounts That Wanna Make Some Money ... I Do All Acco unts . I Do Edd , SBA . loans & Etc .
 NoCapKennels > RunUp BagsDaily 2021-11-15 7:48:48 (UTC)	U fw edd too? LINKS IN THIS MESSAGE 
 FreeBigLo > RunUp BagsDaily 2021-12-13 4:45:57 (UTC)	EDD back green? LINKS IN THIS MESSAGE 
 tha.realnae > RunUp BagsDaily 2022-01-12 21:23:56 (UTC)	The bank or the edd ! I want you to do my shit ion need nobody knowing my SSN 😂
 Casshay Holmes > RunUp BagsDaily 2022-01-19 8:19:39 (UTC)	Edd
 \$moochie\$ > RunUp BagsDaily 2022-01-19 8:19:52 (UTC)	Edd

Possession of firearms

19. While reviewing the Instagram return for “runupbagsdaily”, Investigators immediately noticed lots of photos of DOWL-EAST with numerous types of firearms. Throughout the entire Instagram return, DOWL-EAST can be seen with firearms on his lap while he drives, in his pockets while he poses for pictures and firearms in his hands posing and aiming at the camera.

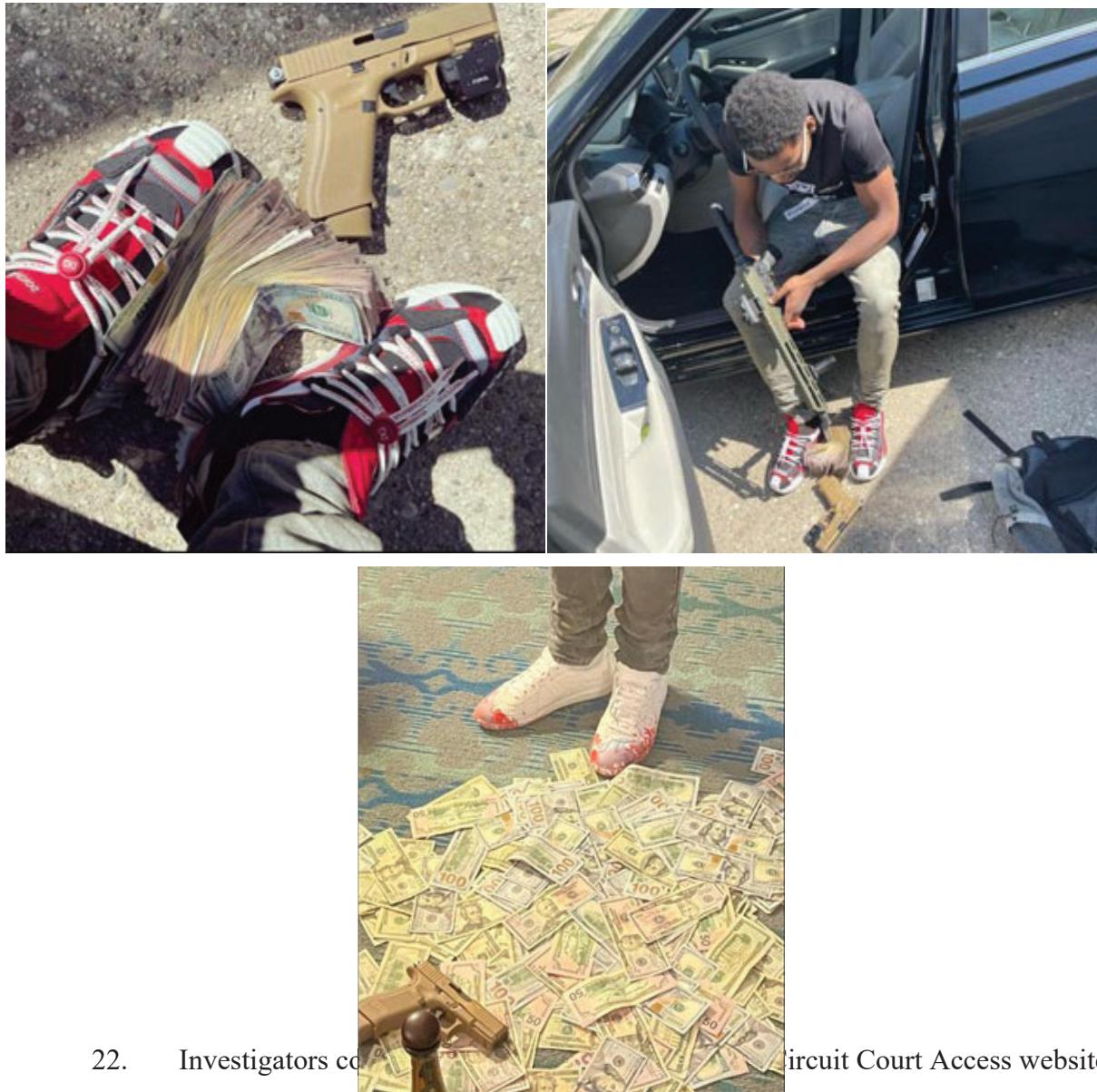
20. Specifically, DOWL-EAST posted several pictures of himself with firearms which displayed the serial number of the firearm in plain view. On or about July 29, 2022, DOWL-EAST posted a picture of himself in his car, with two firearms on his lap. The top firearm appeared to be a Glock style pistol, which serial number was visible and read “ASPM151”. The bottom firearm, which also appeared to be a Glock style pistol, appeared to

have a full auto sear affixed to the back plate of the firearm. It should be noted that the addition of an auto sear converts the semi-automatic pistol into a machinegun under the National Firearms Act. A screen shot is set forth below.



21. Investigators identified several firearms which possessed what appeared to be a

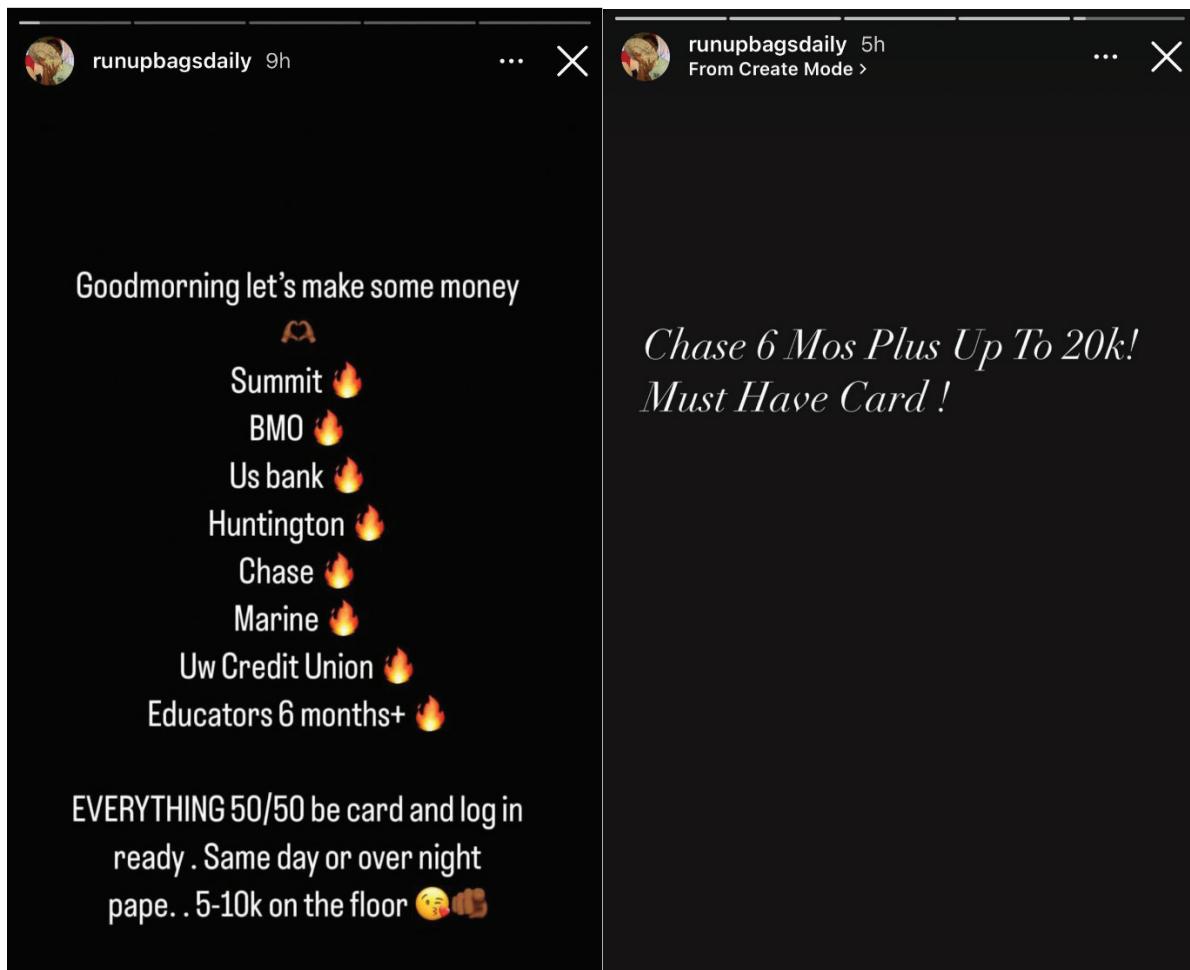
full-auto sear affixed to the backplate of the firearm, rendering them machineguns. Below are three (3) photographs pulled from his Instagram page which showed DOWL-EAST with large sums of cash, a rifle and a tan colored Glock style pistol with what appears to be an affixed auto sear. The photographs were posted between May 1, 2021 and May 2, 2021.



and discovered that DOWL-EAST was convicted of a Felony on September 5, 2017, related to Milwaukee County Case Number 2017CF001436. Due to DOWL-EAST's Felony conviction, he is prohibited from possessing firearms or ammunition. Investigations believe there is probable cause to believe that the firearms depicted on DOWL-EAST's Instagram are real due to serial numbers matching those of real firearms and the fact that facsimile firearms do not have the ability to add a full auto sear to the backplate.

Identification of Sidney Place Address

23. Case agents continued to monitor the Instagram account, "runupbagsdaily", which they knew was owned and operated by DOWL-EAST. Once DOWL-EAST was arrested in August of 2022, his account stopped posting for a short period of time but the account quickly started posting again. The posts, once again were soliciting others, asking people if they wanted to make easy money. Set forth below are screen shots from December 1, 2022, from the Instagram account, "runupbagsdaily".



24. Investigators conducted an analysis on the Instagram account, “runupbagsdaily” and subpoenaed the IP addresses that most frequently accessed this Instagram account. Investigators served a subpoena on AT&T U-verse for subscriber information pertaining to a static IP address utilized to access the Instagram account “runupbagsdaily”. The IP address utilized to access the Instagram account was “104.48.39.10”. AT&T U-verse identified the subscriber for the account that accessed the Instagram as of December 2022, was Brianna EALY,

with a service address of 6554 N Sidney Place, Apartment 202, Glendale, WI 53209, phone number of 262-239-1234.

25. A subpoena was served on Sidney Place Apartments, LLC for tenant information for 6554 N Sidney Place, Apt. 202, Glendale, WI 53209. The company returned the lease agreement for the apartment which showed it was rented to BRIANNA EALY and she had been renting that apartment since June 25, 2022.

26. Agents checked the jail message program where DOWL-EAST is incarcerated, and there were approximately 1,287 messages and over 1,000 phone calls between DOWL-EAST and EALY, many of which from his July arrest date to the present. In the jail conversations, DOWL-EAST and EALY talk about currently having children together and EALY's wavering allegiance to DOWL-EAST depending on how long he is going to be in jail. The latest conversation was on May 3, 2023. Additionally, case agents reviewed DOWL-EAST's commissary account and determined that EALY made 25 deposits, totaling \$1,231 dollars for charges on his tablet.

27. On February 19, 2023, EALY sent a picture to DOWL-EAST in jail which showed one of their children holding a large sum of money. A screen shot is set forth below.



28. Case agents reviewed jail messages between DOWL-EAST and EALY, several of the messages between the two discussed large sums of money, alluding to the fact that DOWL-EAST had sums of money at the time he was arrested on August 18, 2022. DOWL-EAST and EALY exchanged several messages on August 20, 2022, pertaining to this money. In summary EALY offered to buy a safe, collect DOWL-EAST's money, and keep it at her house. DOWL-EAST agreed to the plan, said he will tell the person with his money the plan and instructed EALY to be careful and not allow people at the house.

29. The discussions about money between DOWL-EAST and EALY continue via jail messages. By example, on March 23, 2023, DOWL-EAST and EALY exchanged several messages arguing about EALY spending money. DOWL-EAST referred to having somewhere between \$45,000 and \$51,000. He was upset and believed EALY spent \$17,000 of the money which EALY denied.

30. Based on these messages affiant believes that after being taken into custody DOWL-EAST facilitated EALY taking custody of and stashing his money with her. Affiant believes that due to the argument about her spending his money that the plan came to fruition and was not just talk.

The Premises to be Searched

31. According to records from AT&T U-verse, Brianna EALY is the account holder for internet supplied to the PREMISES. According to public records checks with the Wisconsin Department of Transportation, Briana EALY's address on file is listed as the PREMISES. Surveillance conducted from April through May 2023 showed EALY leaving the PREMISES on several occasions.

32. There is probable cause to believe that evidence and fruits of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C. § 1343 (wire fraud), will be located at the PREMISES occupied by Brianna EALY.

TECHNICAL TERMS

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

34. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

35. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being

used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

36. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of

session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created.

The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on

the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

37. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be

unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

38. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a

later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

39. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

The property to be searched 6554 N Sidney Place, Apt. 202, Glendale, WI 53209, pictured below:



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(g)(1) (possession of a firearm by a felon), and 18 U.S.C. § 1343 (wire fraud), involving Zariyus DOWL-EAST and Brianna EALY, and occurring after July 1, 2020 including:
 - a. Large quantities of U.S. currency;
 - b. Records and information relating to the creation and use of counterfeit checks;
 - c. Firearms and/or ammunition;
 - d. Records and information relating to a conspiracy to defraud the government;
 - e. Records and information relating to an access of US currency fraudulently obtained using another individual's identity;
 - f. Records and information relating to COVID-19 relief;
 - g. Records and information relating utility bills, writings, cell phones, computers, receipts, notes, ledgers, receipts and/or other documentary evidence establishing who is in control of the premises; and
 - h. Records and information relating to the identity or location of the suspects;
2. Computers or storage media used to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

May 10, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address)
 The property located at 6554 N Sidney Place,)
 Apt. 202, Glendale, WI 53209.)
)
) Case No. 23 MJ 85

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin (identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 5/24/2023 (not to exceed 14 days) in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. William E Duffin (United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for _____ days (not to exceed 30) until, the facts justifying, the later specific date of _____.

Date and time issued: 5/10/2023 at 11:48 AM


Judge's signature

City and state: Milwaukee, WI

 Hon. William E Duffin, U.S. Magistrate Judge
 Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched 6554 N Sidney Place, Apt. 202, Glendale, WI 53209, pictured below:



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(g)(1) (possession of a firearm by a felon), and 18 U.S.C. § 1343 (wire fraud), involving Zariyus DOWL-EAST and Brianna EALY, and occurring after July 1, 2020 including:
 - a. Large quantities of U.S. currency;
 - b. Records and information relating to the creation and use of counterfeit checks;
 - c. Firearms and/or ammunition;
 - d. Records and information relating to a conspiracy to defraud the government;
 - e. Records and information relating to an access of US currency fraudulently obtained using another individual's identity;
 - f. Records and information relating to COVID-19 relief;
 - g. Records and information relating utility bills, writings, cell phones, computers, receipts, notes, ledgers, receipts and/or other documentary evidence establishing who is in control of the premises; and
 - h. Records and information relating to the identity or location of the suspects;
2. Computers or storage media used to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.